

REMARKS*Claim Amendments*

Applicants respectfully request entry of the foregoing claim amendments, which amend Claims 1, 4, 13-15, 20, 23, 31-33, 38, 40 and 41 in order to clarify the claimed invention and place those claims in better condition for appeal. Support for the claim amendments can be found at Page 2, lines 21-24; Page 5, lines 17-20; Page 7, lines 17-21; Page 7, line 26 to Page 9, line 23; and Page 12, lines 15-17, among other places. No new matter is introduced.

Rejections under 35 U.S.C. §103

Claims 1-2, 7-8, 16-21, 25-26 and 34-37 are rejected under 35 U.S.C. §103 due to U.S. Pat. No. 6,081,793 of Challener *et al.* (here, “Challener *et al.*”) in view of U.S. Pat. No. 5,903,652 of Mital (here, “Mital”), and further in view of the article “How to Share a Secret” by Adi Shamir, from the *Communications of the ACM*, November 1979, Vol. 22, No. 11 (here, “Shamir”), and further in view of Schneier (“Applied Cryptography,” Second Edition, 1996).

Dependent Claims 4, 9-12, 23 and 27-30 are rejected under 35 U.S.C. §103 due to Challener *et al.* in view of Mital, and further in view of Shamir and Schneier. It is noted that the Office Action refers to a “Stallings” reference as having been cited against Claims 1 and 20; however, no Stallings reference was cited against Claims 1 and 20. Applicants therefore assume that the reference to Stallings is a typographical error, and that the rejection of these dependent Claims is intended to be based on Challener *et al.*, Mital, Shamir and Schneier.

Dependent Claims 13-15, 31-33 and 38 are rejected under 35 U.S.C. §103 due to the same references as in the previous grouping of dependent claims, and further in view of U.S. Patent No. 6,151,631 of Ansell *et al.* (here, “Ansell *et al.*”). Again, the reference to “Stallings” is assumed to be a typographical error.

Dependent Claim 39 is rejected under 35 U.S.C. §103 due to Challener *et al.* in view of Mital and Shamir, and further in view of European Patent EP 0 909 074 A1 of Coss *et al.*

Applicants note that the listing of pending claims on Pages 1 and 2 of the Office Action is incorrect, and that the presently pending claims are 1, 2, 4, 7-21, 23 and 25-41.

Independent Claims 1 and 20

Applicants respectfully submit that Challener *et al.* in view of Mital, and further in view of Shamir and further in view of Schneier does not disclose or suggest the claimed mapping module in combination with the other features of independent Claims 1 and 20, as amended.

Applicants' Claims 1 and 20 involve, among other things, a mapping module that anonymously maps the personal identifier portions of working data so that a receiver obtains anonymous data, while leaving the research data portion unmapped by the anonymous mapping. The identifier portions and the research data portions of the working data are transmitted over a secure communications channel, which is formed by a sender being authenticated with a communication module and a receiver being authenticated with the communication module. Keyholder access to the mapping module is controlled by a secret sharing module.

Such a system may be used, for example, to allow medical records of individuals to be sent to a scientist for a public health study. The medical records initially have personal identifiers, such as the patients' social security identifiers, associated with the medical data that is to be the subject of the scientist's research. By anonymously mapping these personal identifiers, a system according to an embodiment of Claims 1 and 20 allows the scientist to study the research data without being able to access the patients' personal identities.

As a further feature, the anonymous mapping of the personal identifiers in amended Claims 1 and 20 is a one-to-one mapping. This has the advantage, for example, that the scientist may return the anonymous data packets to the original sender, by a reverse mapping, so that the original sender may obtain data that can be identified by personal identifiers. Thus, for example, the scientist could mark records of patients' found to be in an at-risk group for a disease or condition, without knowing the personal identifiers for the individuals in that group; and return all of the records to the original sender with those records marked. The original sender could then contact those individuals to provide medical advice to the at-risk group.

The cited combination of Challener *et al.* in view of Mital, and further in view of Shamir and further in view of Schneier does not disclose or suggest such an apparatus having all of the foregoing components, or the corresponding method of independent Claim 20.

In particular, Challener *et al.* does not disclose or suggest an apparatus or method having the anonymous, one-to-one mapping of amended Claims 1 and 20. Instead, as shown in Fig. 9D,

Challener *et al.* is an automated voting technique in which individuals' votes are ultimately forwarded to a results server with an "add" message. However, the reverse mapping is not possible, since the results server does not receive the voter's ID along with the vote, instead receiving the vote only with an "add" message. Challener *et al.* therefore does not disclose or suggest an anonymous one-to-one mapping, as in amended Claims 1 and 20, along with the other elements of those claims.

Similarly, Mital does not disclose or suggest such an anonymous one-to-one mapping, along with the other elements of amended Claims 1 and 20. Instead, Mital involves a consumer computer 100 sending a secure purchase order message 102 to an electronic commerce service 104. The secure purchase order message 102 includes an auditing attachment, a goods and services order, and payment instructions. The electronic commerce service 104 removes the auditing attachment, and forwards the goods and services order and payment instructions to a merchant computer 108. The merchant computer 108 accesses the goods and services order, and forwards the payment instructions to an acquirer computer 112 in order to obtain payment authorization. Once payment authorization is received, the merchant computer 108 generates a receipt message 116 that is forwarded to the consumer computer 100.

However, in no case does Mital disclose or suggest a sender becoming authenticated with a communications module, and a receiver becoming authenticated with a communications module to create a secure communications channel; and an anonymous, one-to-one mapping transmitting anonymous working data over the secure channel in a reversible fashion. For example, although the electronic commerce service is placed between the consumer computer and the merchant, it does not institute an anonymous, one-to-one mapping between the consumer and the merchant. Instead of being anonymous, the consumer's personal identity is made available to the merchant, so that an order may be associated with the correct shipping information.

Similarly, Shamir does not disclose or suggest a sender becoming authenticated with a communications module, and a receiver becoming authenticated with a communications module to create a secure communications channel; and an anonymous, one-to-one mapping transmitting anonymous working data over the secure channel in a reversible fashion. Instead, Shamir is directed to a technique for secret-sharing.

Likewise, Schneier does not disclose or suggest the anonymous, one-to-one mapping module and other components of Claims 1 and 20. In the cited passage at Pages 54-57 of Schneier, techniques are described by which two parties can authenticate each other; however, these passages do not disclose or suggest the claimed communication module, in which the sender is authenticated with the communication module, and the receiver is authenticated with the communication module, to form a secure channel over which working data is transmitted. Furthermore, Schneier does not disclose or suggest using an anonymous one-to-one mapping to transmit working data anonymously over such a secure channel.

Further, none of the cited combination of references discloses or suggests using secret sharing to control keyholder access to a system having both a communication module that creates a secure channel, and an anonymous, one-to-one mapping of working data between parties over that secure channel.

Therefore, because Challener *et al.* in view of Mital, and further in view of Shamir and further in view of Schneier does not disclose or suggest the inventions of independent Claims 1 and 20, Applicants respectfully request reconsideration and allowance of those claims.

Dependent Claims

In addition, because dependent Claims 2, 4, 7-12, 16-19, 21, 23, 25-30, 34-37, 40 and 41 incorporate the features of base Claims 1 and 20, they are also allowable for the foregoing reasons.

Also, neither Schneier, nor Ansell *et al.*, nor Coss *et al.*, which are applied to the other dependent Claims 13-15, 31-33, 38 and 39, discloses or suggests the foregoing features. In particular, those references do not disclose or suggest the claimed mapping module in combination with the other features of independent Claims 1 and 20.

Applicants therefore submit that all of the dependent Claims are also allowable for the foregoing reasons.

Claims 40 and 41

Claims 40 and 41 were not addressed in the Office Action. Therefore, for the sake of clarity, Applicants submit that Claims 40 and 41 are also allowable for the reasons given above

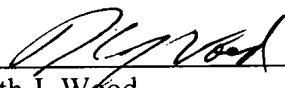
for their respective base Claims 1 and 20, and request reconsideration and allowance of those claims.

CONCLUSION

In view of the above amendments and remarks, it is believed that all claims are in condition for allowance, and it is respectfully requested that the application be passed to issue. If the Examiner feels that a telephone conference would expedite prosecution of this case, the Examiner is invited to call the undersigned.

Respectfully submitted,

HAMILTON, BROOK, SMITH & REYNOLDS, P.C.

By 
Keith J. Wood
Registration No. 45,235
Telephone: (978) 341-0036
Facsimile: (978) 341-0136

Concord, MA 01742-9133

Date: 4/3/07